COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 37, No. 2, 1988

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

Rings Viewed through a Simply Structured Submonoid of Their Unit Groups

by

B. DE LA ROSA, H. FRANCE-JACKSON
and L. C. A. VAN LEEUWEN

(Received April 22, 1988)

§ 1. Introduction

Throughout this paper the symbol A denotes an associative ring with unity $e \neq 0$. $\mathfrak{U}(A)$ denotes the group of units of A; A^o the group of quasi-regular elements of A (under $aob = a+b+ab$); J the Jacobson radical of A; and $\mathrm{char}(A)$ the characteristic of A. $|X|$ designates the cardinality of the set X; ϕ denotes the Euler function; and $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{Z}_n$ have their usual meanings. We set

$$\mathfrak{E}(A) := \{a \in A : ma = e \text{ for some } m = m(a) \in \mathbb{N}\}.$$

It is easily verified that $\mathfrak{E}(A)$ is a submonoid of $\mathfrak{U}(A)$. In Section 2 we determine conditions under which $\mathfrak{E}(A)$ is a subgroup of $\mathfrak{U}(A)$ and we show that this subgroup is a very simply structured one, (Theorems 1, 2 and Corollaries). The section is concluded with the theorem: $\mathfrak{E}(A) = A \setminus \{0\}$ if and only if A is a finite field with prime cardinality. In Section 3 we study the condition $\mathfrak{U}(A) = \mathfrak{E}(A)$ on *artinian* rings A, proceeding through a sequence of auxiliary results to our main result: A ring A is an artinian ring with $\mathfrak{U}(A) = \mathfrak{E}(A)$ if and only if A is isomorphic to a direct sum of the form $\mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{s_n}}$, where $(p_1, \cdots, p_n)$ is a sequence of primes with the properties $(p_i, p_j \text{ odd}, i \neq j) \Rightarrow (p_i, p_j) = 1$ and $(p_i = p_j = 2, i \neq j) \Rightarrow (p_i^{s_i}, p_j^{s_j}) = 2$.

§ 2. Cases where $\mathfrak{E}(A)$ is a subgroup of $\mathfrak{U}(A)$

Let A be an arbitrary (i.e. not necessarily artinian) associative ring with unity $e \neq 0$. The well-known definition of the concept of a nilpotent element a in A comes in the *multiplicative-additive* form

$$a^m = 0 \qquad \text{for some} \quad m = m(a) \in \mathbb{N}.$$

We now reverse the above order of the two operations and consider those elements a in A with the *additive-multiplicative* property

$$ma = e \qquad \text{for some} \quad m = m(a) \in \mathbb{N}.$$

The fundamental object for our study in this paper is the set

$$\mathfrak{E}(A) := \{a \in A : ma = e \text{ for some } m = m(a) \in \mathbb{N}\}.$$

If $a \in \mathfrak{E}(A)$ then $a \neq 0$; and the equalities $(me)a = e = a(me)$ show that $a \in \mathfrak{U}(A)$. Clearly $\mathfrak{E}(A)$ is a submonoid of $\mathfrak{U}(A)$. It is, however, not a subgroup in general, a simple counterexample being $\mathfrak{E}(\mathbb{Q}) = \{1/n : n \in \mathbb{N}\}$ in $\mathfrak{U}(\mathbb{Q}) = \mathbb{Q}\setminus\{0\}$. The purpose of this section is to investigate conditions under which $\mathfrak{E}(A)$ is a subgroup of $\mathfrak{U}(A)$ and to exhibit the structure of $\mathfrak{E}(A)$ in such cases.

For each $a \in \mathfrak{E}(A)$ there is a unique minimal $\mu(a) \in \mathbb{N}$ such that $\mu(a) \cdot a = e$. If $a, b \in \mathfrak{E}(A)$ with $\mu(a) = \mu(b)$, then $\mu(b) \cdot a = e$ implies that $a = (\mu(b) \cdot e)^{-1} = b$. Hence we have that the function

$$\mu : \mathfrak{E}(A) \longrightarrow \mathbb{N}, \qquad a \longmapsto \mu(a)$$

is injective. We shall have occasion to use the properties of this function.

THEOREM 1. *In a ring A, $\mathfrak{E}(A)$ is a subgroup with more than one element of $\mathfrak{U}(A)$ if and only if A has characteristic greater than 2.*

Proof. Suppose that $\operatorname{char}(A) = n > 2$. Since $\mu(a) < n$ for all $a \in \mathfrak{E}(A)$ and since μ is injective, we have that $\mathfrak{E}(A)$ is a finite submonoid of $\mathfrak{U}(A)$, and hence a subgroup. From $(n-1)(-e) = e$, $n-1 > 1$ and $e \neq -e$ it follows that $\mathfrak{E}(A) \neq \{e\}$.

Conversely, suppose that $\mathfrak{E}(A) \leqq \mathfrak{U}(A)$, $\mathfrak{E}(A) \neq \{e\}$. Let $a \in \mathfrak{E}(A)$ with $a \neq e$. Then $ma = e$ for $m = \mu(a) > 1$, and hence $e \neq me = a^{-1} \in \mathfrak{E}(A)$. This ensures the existence of an integer $k > 1$ such that $k(me) = (km)e = e$, so that $(km-1)e = 0$. Since $km - 1 \geqq 3$ we have that $\operatorname{char}(A) \neq 0$. Clearly $\operatorname{char}(A) = 2$ would imply the contradiction $\mathfrak{E}(A) = \{e\}$. □

COROLLARY 1. *If A is a ring with non-zero characteristic then $\mathfrak{E}(A) = \{e\}$ if and only if* $\operatorname{char}(A) = 2$.

For the remaining possible value of the characteristic we prove:

COROLLARY 2. *If A is a ring with zero characteristic then either $\mathfrak{E}(A) = \{e\} \neq \mathfrak{U}(A)$ or $\mathfrak{E}(A)$ is a countably infinite submonoid (and not a subgroup) of $\mathfrak{U}(A)$.*

Proof. $\mathfrak{U}(A) \neq \{e\}$ follows from $e \neq -e \in \mathfrak{U}(A)$. Suppose $\mathfrak{E}(A) \neq \{e\}$. Then, by $\operatorname{char}(A) = 0$ and Theorem 1, $\mathfrak{E}(A)$ is not a subgroup of $\mathfrak{U}(A)$. Hence, since $(\mathfrak{E}(A), \cdot)$ is a monoid, $\mathfrak{E}(A)$ cannot be finite. The result now follows from the injectivity of μ. □

Returning to the case of a ring A with non-zero characteristic we now give an explicit characterization of the subgroup $\mathfrak{E}(A)$.

THEOREM 2. *Let A be a ring with non-zero characteristic n. Then*

$$\mathfrak{E}(A) = \{me : 1 \leqq m < n,\ (m, n) = 1\},$$

(and hence $\mathfrak{E}(A) \cong \mathfrak{U}(\mathbb{Z}_n)$).

Proof. We first show that

(1) $a \in \mathfrak{E}(A) \Rightarrow (\mu(a), n) = 1$.

Let $a \in \mathfrak{E}(A)$ and set $(\mu(a), n) = d$, say $\mu(a) = qd$ and $n = rd$. If $d > 1$ then $r < n$; and $e = \mu(a) \cdot a = (qd)a$ so that $re = q(rd)a = q(na) = 0$, contradicting the definition of n. It follows that $(\mu(a), n) = 1$.

Next we prove that

(2) $(1 \leqq m < n,\ (m, n) = 1) \Rightarrow \exists\, a \in \mathfrak{E}(A) \ni m = \mu(a)$.

If $(m, n) = 1$ there are integers u, v such that $mu + nv = 1$, from which it follows that $m(ue) = e$. Thus we have that $ue \in \mathfrak{E}(A)$. If $m \neq \mu(ue)$ then $m > \mu(ue) = m'$, say; and $m = m' + w$, $0 < w < n$. From $m(ue) = m'(ue) + w(ue)$ we obtain $w(ue) = 0$, i.e. $(we)(ue) = 0$. Since $ue \in \mathfrak{E}(A)$ it follows that $we = 0 \cdot (ue)^{-1} = 0$, contradicting the definition of n. Hence $m = \mu(ue)$.

By (1) and (2) we have that

$$\{\mu(a) \cdot e = a^{-1} : a \in \mathfrak{E}(A)\} = \{me : 1 \leqq m < n,\ (m, n) = 1\};$$

and the result follows from the injectivity of μ. □

Employing Corollaries 1 and 2 on the one hand, and Corollary 2 and Theorem 2 on the other, we have:

COROLLARY 3. *Let A be a ring in which $\mathfrak{E}(A)$ is a subgroup of $\mathfrak{U}(A)$. Then*

(1) $\mathfrak{E}(A) = \{e\}$ *if and only if either* $\mathrm{char}(A) = 0$ *or* $\mathrm{char}(A) = 2$.

(2) $\mathfrak{E}(A)$ *is a finite group.*

Beside the already considered critical condition $\mathfrak{E}(A) = \{e\}$ we shall consider two more: we conclude this section with considering $\mathfrak{E}(A) = A \setminus \{0\}$, and reserve the more general condition $\mathfrak{E}(A) = \mathfrak{U}(A)$ for a study of artinian rings in Section 3.

THEOREM 3. *Let A be a ring. Then $\mathfrak{E}(A) = A \setminus \{0\}$ if and only if A is a finite field with prime cardinality.*

Proof. If $A \cong \mathbb{Z}_p$ for a prime p, then $\mathfrak{E}(A) \cong \mathfrak{E}(\mathbb{Z}_p) = \mathfrak{U}(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\}$.

Conversely, let $\mathfrak{E}(A) = A \setminus \{0\}$. Then $\mathfrak{E}(A) = \mathfrak{U}(A)$. If $\mathfrak{E}(A) = \mathfrak{U}(A) = \{e\}$ then $A \cong \mathbb{Z}_2$. Suppose that $\mathfrak{E}(A) = \mathfrak{U}(A) \neq \{e\}$. Then (by Theorem 1) A is a ring with non-zero characteristic, n, say. Now our hypothesis and Theorem 2 show that A is a finite ring with $\phi(n) + 1$ elements. If k is a divisor of n with $1 < k < n$, then $0 \neq ke \in A \setminus \{0\} = \mathfrak{E}(A)$. But then, again by Theorem 2, $(k, n) = 1$, a contradiction. Hence n is a prime, and $|A| = \phi(n) + 1 = n$. Finally, if $0 \neq a, b \in A$, then $ab \in \mathfrak{U}(A)$ so that $ab \neq 0$. Thus we have that A is a finite domain, and hence a division ring, and hence a field (Wedderburn). □

§ 3. A structure theorem for artinian rings with unity

We now turn to a study of the critical condition $\mathfrak{U}(A) = \mathfrak{E}(A)$. From Theorem 1 and Corollaries 1 and 2 we see that this condition holds only if the ring A has non-

zero characteristic. Theorem 2 therefore defines our scope to be the class of rings A satisfying the condition $\mathfrak{U}(A) \cong \mathfrak{U}(\mathbb{Z}_k)$, where $k = \text{char}(A)$. Our purpose in this section to give a complete characterization of the (left) *artinian* rings in this class.

We begin by considering the equality $\mathfrak{U}(A) = \mathfrak{E}(A)$ in rings of the form $A = \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_n}$, where the k_i are arbitrary positive integers $\geqq 2$. If, however, k has the prime decomposition $k = p_1^{t_1} \cdots p_r^{t_r}$, then $\mathbb{Z}_k \cong \mathbb{Z}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{t_r}}$. In view of this we may restrict our attention to the case where the k_i are prime powers. We prove the (for our purposes) fundamental:

LEMMA 1. *Let $A = \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_n}$, where $k_i = p_i^{t_i}$, p_i prime, $t_i \geqq 1$, $i = 1, \cdots, n$. Then $\mathfrak{U}(A) = \mathfrak{E}(A)$ if and only if the following two conditions hold:*

(1) *If k_i and k_j are both odd for $i \neq j$, then $(k_i, k_j) = 1$.*

(2) *If k_i and k_j are both even for $i \neq j$, then $(k_i, k_j) = 2$.*

Proof. $\mathfrak{U}(A) = \mathfrak{E}(A)$ if and only if for any element $(\bar{a}_1, \cdots, \bar{a}_n) \in \mathfrak{U}(A)$ there exists an $m \in \mathbb{N}$ such that $m\bar{a}_i = \bar{1}$ in $\mathbb{Z}_{k_i}$, $i = 1, \cdots, n$.

Now assume that $\mathfrak{U}(A) = \mathfrak{E}(A)$. Suppose that k_i and k_j are both odd, $i \neq j$. Then $(\bar{a}_1, \cdots, \bar{a}_n)$ with $\bar{a}_i = \bar{2} \in \mathbb{Z}_{k_i}$ and $\bar{a}_s = \bar{1} \in \mathbb{Z}_{k_s}$ for $s \neq i$ is in $\mathfrak{U}(A)$. Hence there is an $m \in \mathbb{N}$ such that $2m \equiv 1 \pmod{k_i}$ and $m \equiv 1 \pmod{k_j}$. But then $2m \equiv 2 \equiv 1 \pmod{(k_i, k_j)}$, and hence $1 \equiv 0 \pmod{(k_i, k_j)}$, i.e. $(k_i, k_j) = 1$. Suppose that k_i and k_j are both even, say $k_i = 2x_i$ and $k_j = 2x_j$. Then $(\bar{c}_1, \cdots, \bar{c}_n)$ with $\bar{c}_i = \overline{2x_i - 1} \in \mathbb{Z}_{k_i}$ and $\bar{c}_s = \bar{1} \in \mathbb{Z}_{k_s}$ for $s \neq i$ is in $\mathfrak{U}(A)$. Hence there is a $y \in \mathbb{N}$ such that $y(2x_i - 1) \equiv 1 \pmod{2x_i}$ and $y \equiv 1 \pmod{2x_j}$. The first of the two congruences here is equivalent with $y \equiv 2x_i - 1 \pmod{2x_i}$, which, together with $y \equiv 1 \pmod{2x_j}$, implies that $2x_i - 2 \equiv 0 \pmod{(2x_i, 2x_j)}$. Hence we have that $(x_i, x_j) \mid x_i - 1$, so that $(x_i, x_j) = 1$; and $(k_i, k_j) = 2$.

Conversely, let (1) and (2) be satisfied. We shall make use of the following theorem from Number Theory, (cf. e.g. [6]): "The system of congruences $z \equiv b_i \pmod{w_i}$, $i = 1, \cdots, n$ is solvable if and only if $(w_i, w_j) \mid b_i - b_j$ for each pair i, j". Let $(\bar{a}_1, \cdots, \bar{a}_n) \in \mathfrak{U}(A)$. Set $(\bar{a}_i)^{-1} = \bar{q}_i$ in $\mathbb{Z}_{k_i}$, $i = 1, \cdots, n$. Consider the system of congruences

$$(*) \qquad z \equiv q_i \pmod{k_i}, \qquad i = 1, \cdots, n$$

and an arbitrary pair i, j. If k_i and k_j are both odd, then $(k_i, k_j) = 1$, and $(k_i, k_j) \mid q_i - q_j$ is satisfied. Suppose that k_i and k_j are both even. Then $(k_i, k_j) = 2$. Since $(a_i, k_i) = (a_j, k_j) = 1$ we have that q_i and q_j are odd numbers. Hence $(k_i, k_j) \mid q_i - q_j$ is satisfied also in this case. The system $(*)$ therefore has a solution z, which may clearly be taken positive. We now have that $za_i \equiv q_i a_i \equiv 1 \pmod{k_i}$, or, equivalently, $z\bar{a}_i = \bar{1}$ in $\mathbb{Z}_{k_i}$, $i = 1, \cdots, n$. □

For ease of reference we emphasize a second auxiliary result on direct sums, this time for general summands.

LEMMA 2. *If $(A_i)_{1 \leqq i \leqq n}$ is a family of rings with unities, then $\mathfrak{U}(A_1 \oplus \cdots \oplus A_n) = \mathfrak{E}(A_1 \oplus \cdots \oplus A_n)$ implies that $\mathfrak{U}(A_i) = \mathfrak{E}(A_i)$, $i = 1, \cdots, n$.*

Proof. If $\mathfrak{E}(A_j) \subset \mathfrak{U}(A_j)$ for some j, a contradiction is provided by

$$\times \mathfrak{U}(A_i) = \mathfrak{U}(\oplus A_i) = \mathfrak{E}(\oplus A_i) \subseteq \oplus \mathfrak{E}(A_i) = \times \mathfrak{E}(A_i) \subset \times \mathfrak{U}(A_i) . \quad \square$$

One more lemma is needed before we can prove our first explicit result on artinian rings A with $\mathfrak{U}(A) = \mathfrak{E}(A)$.

LEMMA 3. *Let A be an artinian ring. Then $\mathfrak{U}(A) = \mathfrak{E}(A)$ implies that $A/J \cong \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_n}$ where $(p_1, \cdots, p_n)$ is a sequence of primes satisfying $(p_i, p_j$ odd, $i \neq j) \Rightarrow (p_i, p_j) = 1$, but which may contain the prime 2 more than once.*

Proof. Since $\mathrm{char}(A) \neq 0$, $\mathfrak{U}(A)$ is a finite abelian group (Theorem 2); and so is therefore A^o in view of $A^o \cong \mathfrak{U}(A)$. Hence, applying Theorem 1 in [2], we have that

$$A/J \cong M_1 \oplus \cdots \oplus M_n$$

where each M_i is either a field or the ring T of 2×2 matrices over $\mathbb{Z}_2$. Now the isomorphisms

$$A^o/J^o \cong (A/J)^o \cong M_1^o \times \cdots \times M_n^o$$

show that the possible summands T must have T^o abelian, which is impossible since T^o is isomorphic to the symmetric group S_3, (cf. [1]). Hence each M_i is a field. From $\mathfrak{U}(A) = \mathfrak{E}(A)$ it readily follows that $\mathfrak{U}(A/J) = \mathfrak{E}(A/J)$, i.e. $\mathfrak{U}(M_1 \oplus \cdots \oplus M_n) = \mathfrak{E}(M_1 \oplus \cdots \oplus M_n)$. By Lemma 2 we have that $\mathfrak{U}(M_i) = \mathfrak{E}(M_i)$, $i = 1, \cdots, n$; and hence (by Theorem 3) that each M_i is a finite field with prime cardinality, say p_i. Hence $M_i \cong \mathbb{Z}_{p_i}$, $i = 1, \cdots, n$; and the equality $\mathfrak{U}(\oplus \mathbb{Z}_{p_i}) = \mathfrak{E}(\oplus \mathbb{Z}_{p_i})$ yields the result in view of Lemma 1. $\square$

We can now prove:

THEOREM 4. *An artinian ring A with $\mathfrak{U}(A) = \mathfrak{E}(A)$ is necessarily finite and commutative.*

Proof. $\mathrm{char}(A) \neq 0$, and hence $|\mathfrak{E}(A)| = \phi(\mathrm{char}(A))$, (Theorem 2). Thus we have that $\mathfrak{U}(A)$ is finite; and this implies (cf. e.g. [7]) the finiteness of A.

By Lemma 3, $A/J \cong \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_n}$ where $(p_1, \cdots, p_n)$ is a sequence of primes. Set $k = \text{l.c.m.}(p_1 - 1, \cdots, p_n - 1)$. Then $k \geqq 1$, and, applying Fermat's Little Theorem to the non-zero coordinates of the images in $\mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_n}$, we find that $a^{k+1} - a \in J$ for all $a \in A$. For each $j \in J$, $e + j \in \mathfrak{U}(A) = \mathfrak{E}(A)$ and hence, (by Theorem 2), $e + j$ is in the center of A for every $j \in J$. This shows that J is contained in the center of A; and so is therefore $a^{k+1} - a$ for every $a \in A$. The commutativity of A now follows from a well-known commutativity theorem (cf. [4], Theorem 3.2.3). $\square$

Remark. The finiteness of A easily follows within our context. In fact, $1 \leqq |J| < \infty$ follows from $|J| = |J^o|$, $J^o \leqq A^o \cong \mathfrak{U}(A) = \mathfrak{E}(A)$ and $|\mathfrak{E}(A)| = \phi(\mathrm{char}(A))$; while $|A/J| < \infty$ is immediate by Lemma 3.

We shall need two preliminary characterizations before we come to our main

result. These form the contents of our two final lemmas.

LEMMA 4. *An artinian ring A with* $\mathrm{char}(A)=m=p_1^{s_1}\cdots p_n^{s_n}$ *is isomorphic to* $\mathbb{Z}_m$ *if and only if it satisfies the two conditions*:

(1) $\mathfrak{U}(A)=\mathfrak{E}(A)$ *and* (2) $A/J\cong\mathbb{Z}_{p_1}\oplus\cdots\oplus\mathbb{Z}_{p_n}$.

Proof. Let $A\cong\mathbb{Z}_m$. Then $\mathfrak{U}(A)\cong\mathfrak{U}(\mathbb{Z}_m)=\{\bar{r}\in\mathbb{Z}_m\colon 1\leqq r<m,\ (r,m)=1\}$, which (by Theorem 2) is isomorphic to $\mathfrak{E}(A)$. To prove (2) we note that $A=\{e, 2e, \cdots, (m-1)e, me=0\}$ and that the homomorphism

$$\psi\colon A/J\to\mathbb{Z}_{p_1}\oplus\cdots\oplus\mathbb{Z}_{p_n},\quad \psi(se+J)=s(\bar{1},\cdots,\bar{1}),\quad s=1,\cdots,m$$

is surjective. Now

$$s(\bar{1},\cdots,\bar{1})=(\bar{0},\cdots,\bar{0})\Rightarrow p_1\cdots p_n\,|\,s\Rightarrow se\in(p_1\cdots p_n)A\subseteq J\,.$$

Thus we have that ψ is an isomorphism.

Conversely, assume (1) and (2). The set

$$\mathfrak{C}=\{te+J\colon t\in T=\{1, 2, \cdots, p_1\cdots p_n\}\}$$

is a complete system of residue classes modulo J in A—this follows from (2) and the fact that $(t-t')(\bar{1},\cdots,\bar{1})$ cannot be zero for $t\neq t'$ in T. Since

$$\mathfrak{U}(A)=\bigcup\{te+J\colon te+J \text{ contains a unit of } A\}\,,$$

(cf. [3] (H)(a), p. 319), and since for a positive integer u, $(u,p_1\cdots p_n)=1\Leftrightarrow(u,m)=1$, the residue classes in $\mathfrak{C}$ consisting of units of A are exactly the $\phi(p_1\cdots p_n)$ classes $te+J$ with $(t,p_1\cdots p_n)=1$, (by (1) and Theorem 2). Hence we must have that $\phi(p_1\cdots p_n)\,|J|=\phi(m)$, so that $|J|=\prod_{i=1}^{n}p_i^{s_i-1}$. Now $A=\bigcup\{te+J\colon t\in T\}$ shows that $|A|=(p_1\cdots p_n)\prod_{i=1}^{n}p_i^{s_i-1}=m$; and hence $A=\{e, 2e, \cdots, (m-1)e, me=0\}\cong\mathbb{Z}_m$. □

LEMMA 5. *A is a finite commutative local ring with $\mathfrak{U}(A)=\mathfrak{E}(A)$ if and only if $A\cong\mathbb{Z}_{p^k}$ for some prime p and some positive integer k.*

Proof. If $A\cong\mathbb{Z}_{p^k}$ then A clearly has the first three properties stated; and the equality $\mathfrak{U}(A)=\mathfrak{E}(A)$ is a direct consequence of Lemma 4.

Conversely, let A be a finite commutative local ring with $\mathfrak{U}(A)=\mathfrak{E}(A)$. Denote by M the set of zero-divisors of A. If $M=\{0\}$, A is a finite field; and now $\mathfrak{E}(A)=\mathfrak{U}(A)=A\backslash\{0\}$ (together with Theorem 3) shows that $A\cong\mathbb{Z}_p$ for some prime p. Suppose that $M\neq\{0\}$. Since A is a finite ring (with unity) one easily finds that $M=A\backslash\mathfrak{U}(A)=\{a\in A:$ a is nilpotent$\}$. The latter form of M shows that (in view of the commutativity of A) M is an ideal of A, and $M=A\backslash\mathfrak{U}(A)$ is therefore the unique maximal ideal of A, so that J is in fact the nilpotent ideal M. Now A/J is a finite field, and from $\mathfrak{U}(A)=\mathfrak{E}(A)$ we have (by Lemma 3) that $A/J\cong\mathbb{Z}_p$ for some prime p. It follows that pe belongs to the nil ideal J, so that the additive order of e is p^k for some positive integer k, and thus $\mathrm{char}(A)=p^k$. It follows (by Lemma 4) that $A\cong\mathbb{Z}_{p^k}$. □

We are now ready to prove our main result in which we characterize all artinian rings A having a fair group of units in the sense that $\mathfrak{U}(A)=\mathfrak{E}(A)$.

THEOREM 5. *A ring A is an artinian ring (with unity) with $\mathfrak{U}(A)=\mathfrak{E}(A)$ if and only if A is isomorphic to a direct sum of the form $\mathbb{Z}_{p_1^{s_1}}\oplus\cdots\oplus\mathbb{Z}_{p_n^{s_n}}$, where $(p_1,\cdots,p_n)$ is a sequence of primes with the properties $(p_i,\ p_j$ odd, $i\neq j)\Rightarrow(p_i,p_j)=1$ and $(p_i=p_j=2,\ i\neq j)\Rightarrow(p_i^{s_i},p_j^{s_j})=2$.*

Proof. Let A be an artinian ring with $\mathfrak{U}(A)=\mathfrak{E}(A)$. Then A is finite and commutative (Theorem 4). Therefore (cf. [5], Theorem 7.13) $A\cong A_1\oplus\cdots\oplus A_n$, where the A_i are finite commutative local rings. Using Lemma 2 we see that $\mathfrak{U}(A_i)=\mathfrak{E}(A_i)$, $i=1,\cdots,n$. Hence (by Lemma 5) each A_i is isomorphic to a $\mathbb{Z}_{p_i^{s_i}}$ for some prime p_i and some positive integer s_i. Now (in view of Lemma 1) the equality $\mathfrak{U}(\oplus\,\mathbb{Z}_{p_i^{s_i}})=\mathfrak{E}(\oplus\,\mathbb{Z}_{p_i^{s_i}})$ forces the primes p_i to have the properties stated.

The converse claim is an immediate consequence of Lemma 1. □

References

[1] ARTIN, E.; *Geometric Algebra*, Interscience Publishers, Inc., 1957.

[2] ELDRIDGE, K. E.; On Ring Structures determined by Groups, *Proc. Amer. Math. Soc.*, **23** (1969), 472–477.

[3] FUCHS, L.; *Infinite Abelian Groups*, Vol. II, Academic Press, 1973.

[4] HERSTEIN, I. N.; *Noncommutative Rings*, The Carus Mathematical Monographs, M.A.A., 1968.

[5] JACOBSON, N.; *Basic Algebra II*, W. H. Freeman and Co., 1980.

[6] LE VEQUE, W. J.; *Topics in Number Theory*, Vol. I, Addison-Wesley Publ. Co., 1956.

[7] STEWART, I.; Finite Rings with a Specified Group of Units, *Math. Z.*, **126** (1972), 51–58.

Department of Mathematics
University of the Orange Free State
Bloemfontein
Republic of South Africa

Department of Mathematics
Vista University
Port Elizabeth
Republic of South Africa

Department of Mathematics
Rijksuniversiteit Groningen
Groningen
The Netherlands